

REMARKS/ARGUMENTS

Claim 98 is pending in this application. No claim was amended.

35 USC §103(a) Rejection

In the Office Action, the Examiner rejected claim 98 under 35 USC §103(a) as being unpatentable over Ganesan (U.S. Patent Number 5,535,276) (hereinafter referred to as "Ganesan"), in view of Johnson et al. (U.S. Patent Number 5,815,573) (hereinafter referred to as "Johnson") and Matyas et al. (U.S. Patent Number 5,142,578) (hereinafter referred to as "Matyas"). Reconsideration in view of the following remarks is respectfully requested.

I. Claim 98

Independent claim 98 recites, among other elements, a step of "*dividing an exponent of the private key into a most significant portion and a least significant portion.*" This element is not disclosed nor suggested in any of the cited references, alone or in combination. The dividing into a most significant portion and a least significant portion is useful as shown in the specification to make incorrectly decrypted keys well-formed.

The specification shows a method for secure cryptographic key storage, in which a malicious hacker who exhaustively tries all possible PINs to recover a private key will recover *many* candidate private keys, all of them equally plausible but only one of which is correct. The only way the hacker can find out which of these keys is the correct one is to use the keys with an administrative authority, thereby exposing himself as an intruder. Candidate private keys are well-formed so that the attacker will not be able to distinguish them from the correct key. As explained in the specification with respect to specific embodiments, one way to ensure that candidate private keys are well formed is to divide the (correct) private key d into a most significant portion and a least significant portion, d_a and d_b , where the concatenation of d_a and d_b equals d . The most significant portion is then combined with different least significant portions

to form candidate private keys. This ensures that the magnitude of a candidate private key remains smaller than a modulus so that the candidate private key is well-formed.

The Examiner conceded that Ganesan is silent on the element of dividing the key into a most significant and a least significant portion, and cited Johnson as teaching that element.

Johnson teaches a key recovery system that accommodates legitimate concerns of law enforcement officials while at the same time resists attacks by unauthorized parties. Two communicating users Alice and Bob agree upon a randomly generated secret value referred to as the PQR value, from which an encryption key is generated. The PQR value comprises an m-bit P value, an m-bit Q value and an n-bit R value (column 6, lines 54-58). The P value is stored with a first key recovery agent, the Q value is stored with a second key recovery agent, and the R value is kept as a shared secret between Alice and Bob (column 6, lines 61-66, Figure 1). Key recovery agents will reveal P and Q to law enforcement officials upon the presentation of sufficient credentials, who then only need to ascertain the R value using available cryptanalytic means (column 1, lines 64-66). Thus, the system has the effective work factor of an n-bit key to law enforcement officials. If one of the key recovery agents was corrupt and revealed its P value to an attacker, the attacker would still be required to break an (m+n)-bit key not knowing the value of Q nor R (column 14, lines 7-12). Thus, the system has the effective work factor of an (m+n)-bit key to an attacker. Hence, Johnson is concerned with making authorized key recovery feasible, while making decryption by unauthorized third parties infeasible. Thus it is apparent that Johnson does not disclose nor suggest a method for secure cryptographic key storage, much less the claimed step of dividing an exponent of the private key into a most significant portion and a least significant portion.

Finally, Matyas was cited for teaching another element. Matyas teaches a method for generating and distributing a key-encrypting key (KEK) using a public-key cryptographic system (column 4, lines 51-57). Matyas merely uses public and private keys of the public-key cryptographic system, and does not teach a method for secure cryptographic key storage. Thus, it does not appear that Matyas discloses or suggests the claimed element of dividing absent from Ganesan and Johnson.

Applicant submits, for at least the reasons stated above, that the cite references do not render claim 98 obvious. Hence, Applicant submits that claim 98 is patentable over Ganesan, Johnson, and Matyas.

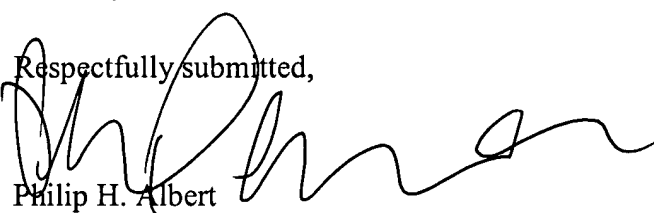
CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 415-576-0200.

Dated: 7/6/04

Respectfully submitted,


Philip H. Albert
Reg. No. 35,819

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 415-576-0200
Fax: 415-576-0300
PHA:jtc
60216788 v1